数理解析研究所講究録 1440 巻 2005 年 1-4

Extremal lattices に付随する球面デザインと extremal modular forms の Fourier 係数の modulo p の性質について（小池正夫、篠原雅史、田上真との共同研究）

坂内 英一　Eiichi Bannai
九大数理　Graduate School of Mathematics, Kyushu University
Hakozaki 6-10-1, Higashi-ku, Fukuoka 812-8581, JAPAN

この原稿は 2004 年 12 月の京大数理研の坂内による上の題での講演の記録です。タイトルの英訳は
"Spherical designs attached to extremal lattices and the modulo p properties of the Fourier coefficients of extremal modular forms (joint work with Masao Koike, Masashi Shinohara and Makoto Tagami) "
であり、坂内、小池、篠原、田上の４名の著者による　このタイトルのプレプリント (投稿中) に基づいています。

講演では、球面デザインの説明からはじめて、even unimodular extremal Euclidean lattices の各 shell （原点からの距離が一定の lattice の元達の作る集合) がユークリッド空間の次元が 24 を法として、0, 8, 16 と合同になるとき (even unimodular lattice の次元は 8 の倍数であることに注意) それぞれ、11-デザイン、7-デザイン、3-デザイン、になるという Venkov の定理を説明し、8 次元の even unimodular lattice である E_8-lattice の shell （それらは全て 7-デザインになるが) のどの１つもが 8-デザインにならないことが、「Ramanujan τ 関数の値 $\tau(m)$ が任意の自然数 m に対して 0 にならない」という整数論における Lehmer の予想と呼ばれる有名な予想と同値になるという Venkov の観察を出発点に、even unimodular extremal Euclidean lattices の各 shell がどのような t に対して、t- デザインになるか（特に Venkov の定理の t よりも大きい t に対して t-デザインになる場合があるか) という問題を考えます。その問題自身は非常に難しくて手が出ないので、１つの even unimodular lattice の全ての shell が Venkov の定理からでてくる t よりも大きい t に対して同時に t- デザインになることがあるかという問題を考え、部分的な結果を得たというのが、この講演の最初の主定理です。Venkov の定理は、コードにたいする Assmus-Mattson 定理の格子に対する類似と考えられますが、実は、binary extremal codes においては、shell （この場合はウエイトが一定のコードの元の集合) が全て同じ t を持っていると言うことが、Bachoc の Assmus-Mattson 定理の（有限群の不変式論と通常の組合せ的デザインの Delsarte の特徴付けを用いた) 別証明から得られるということもこの論文のもう１つの主定理です。（以下の Extended Abstract では最後に Remark として書いてあります。)

さらに、この講演の最初の主定理に関係して、必ずしも lattice のテーター級数から来るとは限らない一般の extremal modular forms （$SL(2,Z)$ に関する) に対してある性質が予想され、それが実際に証明されるというのが、この講演の後半の主定理です。(大雑把に言っ

て、３つのことをこの講演、および上であげたプレプリントで証明しています。）もう少し詳しい解説を、講演に忠実な形で、再現しようとしたのですが、時間が無くなって（すでに報告集の原稿の締めきりに遅れてしまっているので）しまったこともあり、難しくなってしまいました。そのかわり、別のところで講演したときのアブストラクトがあるので、それを添付させていただきます。より詳しい内容を知りたい方は、プレプリントを著者まで請求していただけますようお願いします。

Extended Abstract: Spherical designs attached to extremal lattices and the modulo p properties of the Fourier coefficients of extremal modular forms

Eiichi Bannai, Masao Koike, Masashi Shinohara, Makoto Tagami, all at Kyushu University.

Theorem of Venkov (cf.[5],[6]), which is an analogue of Assmus-Mattson theorem for codes, says that each nontrivial shell of an extremal even unimodular lattice in the Euclidean space $\mathbb{R}^n$ is (at least) a spherical 11-design (resp. 7-design, 3-design) in $\mathbb{R}^n$, if n is a multiple of 24 (resp. congruent to 8 modulo 24, congruent to 16 modulo 24). It is an interesting problem, posed by Venkov, de la Harpe and Pache (cf.[2]), when does it become a t-design, for a bigger value of t than mentioned above. This innocent looking problem is not easy to solve, as it is seen for example from the fact that the statement that no shell of the E_8-lattice can become an 8-design is equivalent to the famous Lehmer's conjecture (cf.[4]) in number theory that the Ramanujan function $\tau(m)$ can never become 0 for any positive integer m.

In the first part of this paper, we consider more specific problem when do all the shells of an even unimodular lattice become t-designs for a bigger value of t than mentioned above. We will show that, when $n \equiv 0 \pmod{24}$ this does not happen in many cases. Namely, we prove the following experimental result:

Theorem 1. Let Λ be an extremal even unimodular lattice in $\mathbb{R}^n$ with $n = 24\mu$. If $\mu \leq 150$ and μ is **not** in B, where $B = \{5, 10, 15, 17, 20, 25, 28, 30, 39, 40, 45, 50, 52, 55, 61, 65, 70, 72, 75, 80, 83, 90, 94, 95, 100, 103, 115, 116, 120, 125, 127, 128, 130, 135, 138, 140, 145, 147, 149, 150\}$, then at least one shell Λ_{2m} of Λ is not a 12-design.

In proving Theorem 1, we use the following:
Fundamental Equation (Venkov [5],[6]). A subset $X(= -X)$ in $S^{n-1}(r)$ is a t-design (where $S^{n-1}(r)$ is the sphere of radius r with the center at the origin) if and only if for all $\alpha \in \mathbb{R}^n$,

$$\frac{1}{|X|}\sum_{x\in X}(\alpha, x)^{2k} = \frac{1\cdot 3\cdot 5\cdot \cdots \cdot (2k-1)}{n(n+2)\cdots(n+2k-2)}(\alpha,\alpha)^k(x,x)^k$$

for all $k = 1, 2, \ldots, [\frac{t}{2}]$.

By taking $k = 6$ and taking α and x from Λ_{2m}, for each $\mu \leq 150$ ($\mu \neq 6$) not in the set B, we can find an odd prime p and m which satisfy the following conditions:

(i) $p|n(n+2)\cdots(n+2k-2)$
(ii) $p \not| 1\cdot 3\cdot 5\cdot \cdots \cdot (2k-1)$
(iii) $p \not| |\Lambda_{2m}|$
(iv) $p \not| m$
The existence of such integer m clearly implies that Λ_{2m} is not a 12-design, by comparing the order of the p-power of both sides of the Fundamental Equation.

The extremal modular form (of weight $k = 12\mu + k_0$ with $k_0 \in \{0, 4, 6, 8, 10, 14\}$) is the modular form

$$f(\tau) = \sum_{m\geq 0} a_m q^m, \quad (q = e^{2\pi i\tau}),$$

with $a_1 = a_2 = \cdots = a_\mu = 0$. (Note that the theta series of an extremal even unimodular lattice in $\mathbb{R}^n$ is the extremal modular form of weight $k = n/2$. Also, note that the extremal modular form exists for each k with k even and ≥ 4, independent of the existence of extremal even unimodular lattices.)

Motivated by Theorem 1, we are interested in studying the modulo p property of the Fourier coefficients of the extremal modular forms. Namely, we are interested in dividing for each pair of k and prime p, which of the following three (exclusive) cases holds:
Case (1) $p|a_i$, for all $i \geq 1$,
Case (2) $p \not| a_i$, for all $i \geq 1$ with $p \not| i$, and there exists at least one $j \geq 1$ with $p \not| a_j$,
Case (3) there exists at least one $j \geq 1$ with $p \not| j$ such that $p \not| a_j$.

We first prove that Case(1) holds, if and only if $(p-1)|k$. (These primes p in Case(1) are called Bernoulli type primes for k.)

We also obtain several conditions which guarantee that Case (2) holds. For example, we prove the following theorem, by using the method of Serre[3].

Theorem 2. Let k_1 to be the number in $\{4, 6, 8, \cdots, p-1, p+1\}$ such that $k \equiv k_1 (\mathrm{mod}\, p-1)$. Let $(p-1) \not| k$. Let l_1 satisfy : $pl_1 \leq \mu+1 < p(l_1+1)$, and let k_2 to be the smallest integer with $k_2 \equiv k_1 (\mathrm{mod}\, p-1)$ and $\dim M_{k_2} \geq l_1+1$. Then r_2 is determined by $k = k_2+(p-1)r_2$. If $r_2 \geq k_2$ holds for p, then the extremal modular form f of weight k is expressed as $f \equiv g(p\tau) (\mathrm{mod}\, p)$, where $g(\tau)$ is the extremal modular form of weight k_2. Moreover, we have $p \mid a_{l_1+1}$.

Theorem 2 is used to prove the following result, which was motivated by Theorem 1. (Note that the the property in Theorem 3 is true for the theta series of extremal even unimodular lattices (by using the theorem of Venkov), but we anticipated that this property may hold for extremal modular forms.

Theorem 3. Let $k = 12\mu$, and let $f_k = 1 + 0\cdot q + 0\cdot q^2 + \cdots + 0\cdot q^\mu + a_{\mu+1}q^{\mu+1} + \cdots$ be the extremal modular form of weight k. Let p be a prime number greater than or equal to 13. Suppose that p divides $2k(2k+2)(2k+4)(2k+6)(2k+8)(2k+12)$. Then Case (2) holds for p, and we get $p|a_{\mu+1}$.

We believe that when p is in Case (2) might be characterized by the following:

Conjecture 4. Let f be the extremal modular form of weight $k = 12\mu$. Suppose that p is in Case (2). (i) Then f is expressed as

$$f(\tau) \equiv g(p\tau) (\mathrm{mod}\ p).$$

for a modular form $g(\tau)$ of smaller weight.
(ii) Moreover, there exist the extremal modular form $g(\tau)$ of a smaller weight, and a natural number r such that

$$f(\tau) \equiv g(p^r\tau) (\mathrm{mod}\ p).$$

(It would be very interesting either to prove or disprove this conjecture. We proved this in many cases, including all the cases of $\mu \leq 150$.)

Remark. We obtained a similar result as Theorem 1 for extremal Type II codes, by using the method of Bachoc[1], which gives an alternative proof of the Assmus-Mattson theorem by using the invariants theory of finite groups. Also, we note that in this code case, we can prove that each nontrivial shell of the code has the constant strength t. However, this property cannnot easily be generalized for extremal lattices so far.

References

[1] C. Bachoc, On harmonic weight enumerators of binary codes. Designs and codes—a memorial tribute to Ed Assmus. Des. Codes Cryptogr. 18 (1999), no. 1-3, 11–28.

[2] C. Pache, Shells of self-dual lattices viewed as spherical designs (preprint, 2004).

[3] J. P. Serre, Congruences et formes modulaires [d'apres H. P. F. Swinnerton-Dyer]. (French) Seminaire Bourbaki, 24e annee (1971/1972), Exp. No. 416, pp. 319–338. Lecture Notes in Math., Vol. 317, Springer, Berlin, 1973.

[4] J. P. Serre, Sur la lacunarite des puissances de η. (French) Glasgow Math. J. 27 (1985), 203–221.

[5] B. B. Venkov, Even unimodular extremal lattices. (Russian) Algebraic geometry and its applications. Trudy Mat. Inst. Steklov. 165 (1984), 43–48.

[6] B. Venkov, Reseaux et designs spheriques. (French) Reseaux euclidiens, designs spheriques et formes modulaires, 10–86, Monogr. Enseign. Math., 37, Enseignement Math., Geneva, 2001.